UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
Western Division

No. 5:15-cv-00068

LUKAS PICK, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. LENOVO (UNITED STATES) INC. and SUPERFISH INC., Defendants.	**CLASS ACTION COMPLAINT FOR DAMAGES** 1) VIOLATION OF THE FEDERAL WIRETAP ACT; 2) TRESPASS TO CHATTELS; 3) VIOLATION OF THE NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT; AND 4) VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW **DEMAND FOR JURY TRIAL**

Plaintiff Lukas Pick ("Plaintiff"), individually and on behalf of a class of all those similarly situated, upon personal knowledge as to facts pertaining to Plaintiff and upon information and belief as to all other matters, based on the investigation of his counsel, against Lenovo (United States) Inc. ("Lenovo") and Superfish Inc. ("Superfish") (collectively, "Defendants") states as follows:

I. NATURE OF THE ACTION

1. It is a rare thing for a market-leading corporation to engage in a systematic course of conduct described as a "catastrophe,"[1] "[r]eckless, careless, and appalling,"[2] and "astoundingly

[1] Joseph Bonneau *et al*., *Lenovo Is Breaking HTTPS Security on its Recent Laptops*, ELECTRONIC FRONTIER FOUNDATION (Feb. 19, 2015), https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops.

[2] David Auerback, *You Had One Job, Lenovo*, SLATE (Feb. 20, 2015 8:23 AM), http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html.

stupid."[3] Rarer still, for a corporation to sink to a level where experts stress, "I cannot understate how evil this is."[4] Defendants shocked the technology world when, on February 18, 2015, it was discovered that Lenovo paired its consumer computers with dangerous and malicious software. Computer Security expert Marc Rogers succinctly summarized Defendants' conduct: "This is unbelievably ignorant and reckless of them. Its [sic] quite possibly the single worst thing I have seen a manufacturer do to its customer base."[5]

2. Defendants intentionally installed "adware" software, known as Superfish Visual Discovery ("Superfish Adware"), on Lenovo computers, thereby intercepting electronic communications sent or received by the computers, from January 1, 2014 through the present, in violation of the Federal Wiretap Act, 18 U.S.C. §2511, *et seq.*, and other related statutes. Lenovo secretly loaded their computers with Superfish Adware, without the consent of purchasing consumers (the "Class"), and subsequently hijacked web sessions, invaded the privacy of the Class, and exposed them to security risks.

3. The Superfish Adware impacted the Class in two significant ways. First, the adware intercepted web sessions and scanned websites that users viewed, later injecting unwanted advertisements in web pages based on the information that was intercepted. Second, and more nefariously, Superfish Adware installed a self-signed root certificate, thereby granting Superfish Adware the same internal security clearance as the software in the computer's operating system. This self-signed root allows Superfish Adware to intercept and decrypt secure requests from HyperText Transfer Protocol Secure ("HTTPS") websites, thereby negating the security features of

---

[3] *Lenovo In Denial: Insists There's No Security Problem With Superfish -- Which Is Very, Very Wrong.*, TECHDIRT (Feb. 19, 2015), https://www.techdirt.com/articles/20150219/10124430071/big-lenono-lenovo-massively-compromises-customers-security-brushes-it-off-as-no-biggie.shtml.

[4] Marc Rogers, *Lenovo installs adware on customer laptops and compromises ALL SSL.*, MARC ROGERS.ORG BLOG (Feb. 19, 2015) http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/.

[5] *Id.*

many banking, remote desktop, tax-filing, and government websites such as the IRS. Even the filing website for this Court uses this HTTPS protocol to enhance the security and integrity of filing.

4. These HTTPS websites use special digital certificates to secure the traffic between users and websites. Lenovo allowed Superfish to install adware that would re-issue those certificates locally on the computer and then "spoof" the real certificate, so they can intercept the once-secure website connection. This is known as a "man-in-the-middle" attack and is viewed as a form of malicious cyber-attack. Most egregiously, Superfish Adware used a simplistic password encryption that some computer experts were able to break in mere minutes, enabling them to spy on any other infected user in the same network and steal their most valuable personal information.[6]

5. Defendants' use of Superfish Adware to inject advertisements in the Internet traffic of the Class has been called "a massive security catastrophe for its users" and "catastrophically irresponsible."[7] Others have noted that "[Superfish Adware] is particularly naughty. People have shown that it can basically intercept everything and it could be really misused."[8] Ken Westin, a senior analyst at cyber security company Tripwire, agreed, adding: "If the findings are true and Lenovo is installing their own self-signed certificates, they have not only betrayed their customers' trust, but also put them at increased risk."[9]

6. On February 19, 2015, as public uproar grew deafening, Lenovo confessed to their intentional use of Superfish Adware to inject advertisements into Internet traffic, and Lenovo Chief Technological Officer ("CTO") Peter Hortensius ("Hortensius") admitted, "We messed up badly

---

[6] Robert Graham, *Extracting the SuperFish certificate*, ERRATA SECURITY BLOG (Feb. 19, 2015) http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html#.VOaDPfnF9fy.

[7] Joseph Bonneau *et al*., *supra* note 1.

[8] Jane Wakefield, *Lenovo taken to task over 'malicious' adware*, BCC (Feb. 19, 2015 7:30 ET) http://www.bbc.com/news/technology-31533028.

[9] *Id.*

here."[10] He also admitted, in an interview with *The Wall Street Journal*, that it was obvious that Lenovo did not do their due diligence by using Superfish Adware.[11]

7. Defendants intentionally released Superfish Adware upon their unsuspecting consumers, trying to make money by intercepting their Internet communication in order to create customized advertisements, but their greedy desire to intercept both secured and unsecured Internet communication triggered public outrage. Defendants forced Class members into an indefensible position: they could no longer trust their secured Internet connections, but, instead, must "trust that this software which has compromised their secure connections is not tampering with the content, or stealing sensitive data such as usernames and passwords," and must further hope that no third party would take advantage of this vulnerability for their own malicious purposes.[12] While operating on Class members' computers, Superfish Adware also slowed down Internet speeds, used limited Internet bandwidth, filled limited hard drive space, and also slowed down system performance by using limited computer resources to process data requests and transfers.

8. As a result of Defendants' unlawful and unfair conduct, Plaintiff, on behalf of himself and members of the Class, brings this action to recover statutory damages, punitive damages, equitable relief, and attorneys' fees and costs under 18 U.S.C. §2511, *et seq.*, Cal. Bus. & Prof. Code §17200, *et seq.*, N.C. Gen. Stat. §75-1.1, *et seq.*, and for Common Law Trespass to Chattels.

---

[10] Jordan Robertson, *Lenovo Apologizes After It 'Messed Up' With Tracking Software*, BLOOMBERG (Feb. 19, 2015 5:03 PM EST) http://www.bloomberg.com/news/articles/2015-02-19/lenovo-says-it-messed-up-by-preloading-web-tracking-software.

[11] Shira Ovide, *Lenovo CTO: We're Working to Wipe Superfish App Off of PCs*, WALL ST. J. L. BLOG (FEB. 19, 2015 3:07 PM ET) http://blogs.wsj.com/digits/2015/02/19/lenovo-cto-were-working-to-wipe-superfish-app-off-of-pcs/.

[12] Graham Cluley, *What You Need to Know About Superfish, The Man-in-the-Middle Adware Installed on Lenovo PCs*, TRIPWIRE (Feb. 19, 2015) http://www.tripwire.com/state-of-security/security-data-protection/superfish-lenovo-adware-faq/.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. §1331 because Plaintiff has alleged the violation of a federal statute, 18 U.S.C. §2511, *et seq*. This Court may also exercise supplemental jurisdiction over the state law claims pled below.

10. This Court has personal jurisdiction over Defendants because they are authorized to do business and in fact do business in this District, Lenovo has its headquarters in this District, Defendants have sufficient minimum contacts with this District, and each Defendant otherwise intentionally avails itself of the markets in this state through the promotion, marketing, and sale of Lenovo products infected with Superfish Adware in this District, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

11. Pursuant to 28 U.S.C. §1391, venue is proper in this District because Lenovo's headquarters is located here, Defendants conduct business in this District, and most events giving rise to Plaintiff's claims arise here.

III. PARTIES

A. Plaintiff

12. Plaintiff Lukas Pick is a resident of San Diego County, California. Plaintiff purchased a Lenovo Yoga 2 Pro from Lenovo during the Class Period as defined herein. Plaintiff used the computer for emails, personal Internet browsing, Internet banking, paying bills, social networking, and completing government forms. Plaintiff did not know that Defendants collected or intercepted his data, nor did Plaintiff authorize Defendants to do so.

B. Defendants

13. Defendant Lenovo (United States) Inc. is a Delaware corporation with its headquarters located in Morrisville, North Carolina. Lenovo is the American subsidiary of Lenovo Group Limited, a Chinese corporation. Lenovo researches, manufactures, and sells personal

computers, business computers, smartphones, tablets, servers, computer hardware, IT management software, televisions, and wearable electronic devices. Since acquiring IBM's personal computer business in 2005, Lenovo has grown to be the largest retailer worldwide in both personal and business computers. For its fiscal year 2013/2014, Lenovo had nearly $39 billion in revenue, 79% of which was derived from the sale of laptop and desktop computers.

14. Defendant Superfish is a Delaware corporation headquartered in Palo Alto, California. Superfish produces both visual search programs and adware. Superfish has produced both software applications that are consensually obtained by consumers, and other adware applications that are surreptitiously downloaded or located within computer hardware. Superfish was founded by its present Chief Executive Officer ("CEO"), Adi Pinhas, a former research analyst at Verint[13] and a co-founder of Vigilant Technologies. Both companies are affiliated closely with military intelligence and surveillance.[14]

IV. FACTUAL STATEMENT

A. Internet Communication and Encryption

15. HyperText Transfer Protocol ("HTTP") is the uniform procedure for exchanging information on the Internet, with standardized sets of commands and codes that all websites follow in order to exchange information with each other and with users. HTTP lacks thorough security features, so there is little to stop an interested party from intercepting electronic communications on the Internet.

---

[13] Verint, founded by ex-intelligence officers, specializes in surveillance and eavesdropping technology. James Bamford, *Shady Companies With Ties to Israel Wiretap the U.S. for the NSA*, WIRED (Apr. 3, 2012 6:30 AM) http://www.wired.com/2012/04/shady-companies-nsa.

[14] Thomas Fox-Brewster, *Superfish: A History Of Malware Complaints And International Surveillance*, FORBES (Feb. 19, 2015 10:37 AM) http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-history-of-malware-and-surveillance/.

16. In order to combat this interception of information, HTTPS was created. HTTPS built upon HTTP by adding a secure link between a server (such as a website) and a client (such as a typical user on the Internet). This link is encrypted by a special and unique security certificate called an SSL Certificate, akin to a password. Without this certificate, any data that is transferred would appear to be incoherent.

17. The following is an example of the difference between an unencrypted and an encrypted message:[15]

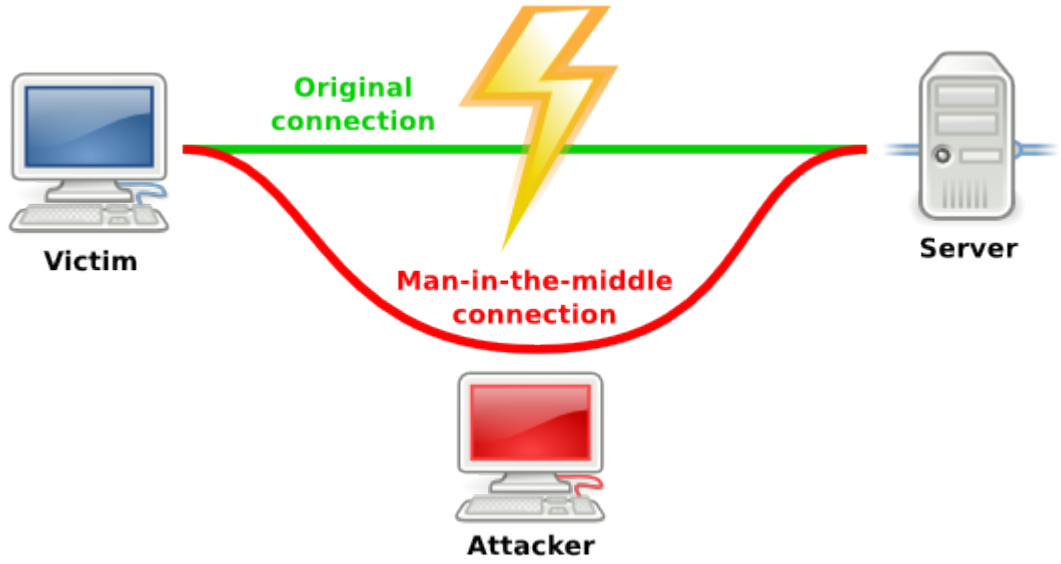
Dear Tim,....pl ease find our r evenues and pro fit statement f or the last bus iness year atta ched. This is c onfidential inf ormation.....Be st regards..	0stkgNGafvEYc3V w1JDkv4PVJ+Lk1H FhSmZgQ2hcjtFF1 ZvkoFu+y3fAUd4L N/q6TrR8YSnL81F idsi16CrN7nMAgB 36mBVL2gL4hYYGh C+z06K+6PJ1WEZX tMONYqZj3PE1whz 8UIZCUsCpnEB

18. This exchange of codes and the encryption and decryption of transferred data occurs behind the scenes whenever a user accesses a website that places particular emphasis on security and privacy. Examples of such websites include online banking, government websites, social networking websites, remote work systems, and even the filing website for this Court.

19. HTTPS provides security sufficient to protect most Internet communication, but it is not invincible. One of the most sophisticated methods to intercept HTTPS is known as a "man-in-the-middle attack," in which a third party attacker forces their way in between the secure connection of the server and the user. If the attacker is able to intercept the secure connection, they are then able to replace the legitimate SSL Certificate with a new, forged SSL Certificate, fooling the user and server into accepting and trusting the connection. With these parties suddenly fooled, their

[15] HTTPS and HTTP Difference, INSTANT SSL, https://www.instantssl.com/https-tutorials/what-is-https.html (last visited Feb. 23, 2015).

communications can be manipulated so that the attacker can view the private data without the aforementioned encryption.[16]



20. A successful man-in-the-middle attack would enable an attacker to have complete and unrestricted access to an affected user's banking sites, personal data, or private messages.[17]

B. The Insidious Effects of Adware

21. Internet advertising is a massive industry that continues to rapidly grow, and capitalizing on that opportunity were many companies that used software known as "adware," also commonly described as a type of malware, short for "malicious software."[18] In contrast to standard Internet advertising, adware is distinguished for its negative effect on consumers. Certain types of adware monitor electronic communication on the Internet, reviewing the actions, searches, and preferences of consumers for later use in targeted advertisement. Other adware directly injects advertisements into a user's Internet websites, and more complicated adware performs both functions simultaneously.

---

16 Graham Cluley, *supra* note 12.
17 Marc Rogers, *supra* note 4.
18 *Id.*

22. Adware and its ilk have not been formally defined by the Federal Trade Commission, but many view the crucial defining characteristics to be the lack of consent and the invasion of privacy that accompany adware. Most users subjected to adware either did not consent to the installation of the program, or the consent was obtained through surreptitious means such as hiding adware within the installation of another computer program. Typical methods of obtaining consent can include mandatory bundling of adware with desired programs, or rearranging the locations of buttons during a program installation to increase the likelihood of accidental acceptance.[19]

23. Sophisticated adware, once installed, performs a series of actions: the adware intercepts a user's actions on the Internet, monitors that activity, submits that information to an external server, processes that information, and then either uses that information to inject special advertisements into websites or sells that information to yet another company. Even if detected, "[o]ften, Adware programs do not have any uninstall procedures and they can use technologies that are similar to those used by viruses to penetrate your computer and run unnoticed."[20]

24. In addition to the irritation provided by injected advertisements and the privacy invasion of adware's Internet traffic interception, adware also negatively impacts the performance of computers. Adware occupies storage space in the limited storage space of a computer's hard drive, and uses some of the computer's limited processing power to execute its commands. Finally, when adware contacts outside servers to transfer intercepted data for analysis and processing, this uses some of the limited Internet bandwidth available to consumers. Injecting additional advertisements into websites similarly increases the Internet traffic on a user's computer, thus slowing overall

---

[19] Barry Leonard, *Spyware Workshop: Monitoring Software on Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*, Diane Publishing Co. (Mar. 2005) http://books.google.co.uk/books?id=ookz_2ONmwgC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

[20] Adware, KASPERKSY LAB, http://usa.kaspersky.com/internet-security-center/threats/adware (last visited Feb. 23, 2015).

operation. These actions have the cumulative effect of slowing the computer's operation, depriving its user of the full effective use of the computer.

25. Superfish has developed and distributed visual search applications since it was founded in 2006 by veterans of the surveillance and eavesdropping industry. However, "Superfish . . . has been criticised by users the world over since its inception in 2006" for its invasive adware and the virus-like characteristics of their adware.[21] Window Shopper, another adware program developed and distributed by Superfish, has yielded frequent comparisons to viruses, with many users confused by its appearance on their computers and equally dismayed by their difficulty removing Window Shopper.[22]

26. Consistent with their prior practices, Superfish developed and distributed Superfish Visual Discovery adware. This adware functions by scanning websites viewed by users, searching for images on the website, analyzing the images on an external server, and then returning to the website to inject new advertisements of other products provided by Superfish affiliates.[23] Superfish would be paid by retailers in exchange for these advertisement views, typically on a per-click or per-view basis. This compensation system is typical of Internet advertising and incentivizes adware producers to maximize clicks and views.

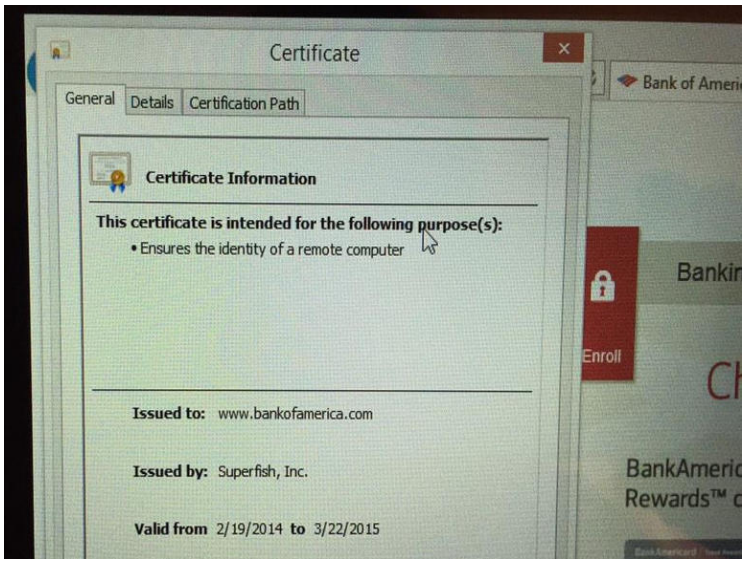
27. To increase user exposure, Superfish made the unprecedented decision to target both HTTP ***and*** HTTPS communication, both for the purposes of injecting advertisements and for the purposes of data interception and analysis. Superfish Adware accomplished this by using man-in-the-middle attacks to replace SSL certificates with their own version of the Certificates.

28. Thus, ***if nothing goes wrong***, Superfish Adware: a) hijacks legitimate connections; b) monitors user activity; c) collects personal information and uploads it to its servers; d) injects

[21] Thomas Fox-Brewster, *supra* note 14.
[22] *Id.*
[23] Jane Wakefield, *supra* note 8.

advertising in legitimate pages; e) displays pop-ups with advertising software; f) uses man-in-the-middle attack techniques to crack open secure connections; and g) presents users with its own fake certificate instead of the legitimate site's certificate.[24]

29. The following is an example of a "spoofed" SSL Certificate for the Bank of America website, issued by Superfish Adware, proving the use of man-in-the-middle attacks:



C. Lenovo Surreptitiously Installed Superfish Adware on Its Computers

30. At some point in 2014, Lenovo partnered with Superfish to install the aforementioned Superfish Adware on their consumer computers. Lenovo then began pre-installing Superfish Adware on Lenovo computers before shipping them to consumers. This enabled Defendants to grant Superfish Adware the same security clearance as operating system software without needing to obtain purchaser consent or without needing to coerce or deceptively obtain consent. When Plaintiff and Class members purchased the computers, Superfish Adware was ***simply there***, but hidden.

31. Although the precise date that Defendants started this practice can only be approximated by Plaintiff, complaints against Superfish Adware emerged in September 2014 on

[24] Marc Rogers, *supra* note 4.

Lenovo websites.[25] Even before realizing the full scope of Superfish Adware's danger, Lenovo customers were furious, drawing comparisons to computer viruses and noting that the act of pre-loading adware was unprecedented among computer manufacturers.

32. Over the next several months, tech-savvy Lenovo customers raised their concerns repeatedly on Lenovo forums, but these complaints were ignored by Defendants.[26] Finally, at least five months after the initial complaints flooded the Lenovo forums, Lenovo responded. A Lenovo forum administrator, Mark Hopkins, stated that "[d]ue to some issues . . . we have temporarily removed Superfish [Adware] from our consumer systems until such time as Superfish [Adware] is able to provide a software build that addresses these issues."[27] He attempted damage control, emphasizing that Superfish Adware was not ***too*** invasive, and claimed that regardless of the level of invasion, all Lenovo customers consented to the adware infection.[28] This appeared to quell some of the purchaser anger, until Google Chrome security engineer Chris Palmer ("Palmer") discovered the full scope of Superfish Adware's danger, and the scale of Lenovo's betrayal of its customers was revealed.

D. Defendants' Practices Prompt Public Outrage

33. Following Twitter conversation about Defendants' use of Superfish Adware, Palmer purchased a Lenovo Yoga 2 Pro to investigate the Superfish Adware. He quickly discovered that Superfish Adware injected itself in HTTPS connections and replaced SSL Certificates, thus compromising the security and safety of ***every single secure website*** accessed by Lenovo's infected customers. Superfish Adware was able to use this attack to intercept all private traffic and then use it

---

[25] Lenovo Community, LENOVO, https://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Lenovo-Pre-instaling-adware-spam-Superfish-powerd-by/td-p/1726839 (last visited Feb. 23, 2015).
[26] Lenovo Community, LENOVO, https://forums.lenovo.com/t5/Security-Malware/Potentially-Unwanted-Program-Superfish-VisualDiscovery/m-p/1860408/highlight/true#M1697 (last visited Feb. 23, 2015).
[27] Lenovo Community, LENOVO, https://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Lenovo-Pre-instaling-adware-spam-Superfish-powerd-by/td-p/1726839/page/3 (last visited Feb. 23, 2015).
[28] *Id.*

to push ads through to these secure websites. Technology websites, blogs, and cyber security experts immediately began investigating Superfish Adware in greater detail.

34. Cyber security experts soon came to a startling revelation: ***every single computer infected by Superfish Adware could be compromised by the same password.*** The CEO of security firm Errata Security, Robert Graham, cracked the Superfish Adware password in mere minutes to demonstrate the danger of Superfish Adware's security breach.[29] Anyone with the password could suddenly wreak havoc on any and all secure information held by Lenovo users on the same network as him. Because Superfish Adware manipulated the "root" of a computer's security certificates, the single most important computer security feature available to consumers, the intrusive power afforded to Superfish Adware was nearly limitless. This same power could be wielded by anyone who held the Superfish Adware password and left infected computers at the mercy of chance. Any competent hacker could obtain all encrypted electronic communication from Lenovo customers, steal passwords, display unwanted web pages, steal encryption keys, and control the user's entire digital experience, all completely undetected.[30]

35. As Defendants' malicious business practices unraveled, Lenovo released an official statement downplaying security concerns and claiming that Superfish Adware was used "to improve the shopping experience."[31] Lenovo added that they shut down the servers Superfish used to run Superfish Adware. Lenovo CTO Hortensius, in an interview with *The Wall Street Journal*, again tried to downplay these risks, vaguely acknowledging a problem and stating "We're not trying to get

---

[29] Robert Graham, supra note 6.

[30] Nicole Perlroth, *Lenovo and Superfish Penetrate the Heart of a Computer's Security*, NY TIMES BLOG (FEB. 22, 2015 5:30 AM), http://bits.blogs.nytimes.com/2015/02/22/lenovo-and-superfish-penetrate-the-heart-of-a-computers-security/?_r=0.

[31] *Lenovo Statement on Superfish*, LENOVO (Feb. 19, 2015) http://news.lenovo.com/article_display.cfm?article_id=1929.

into an argument with the security guys. They're dealing with theoretical concerns."[32] When asked by *The Wall Street Journal*, "Do you do due diligence on software you pre-install on Lenovo machines to make sure it's secure?" Hortensius admitted, "Obviously in this case we didn't do enough."[33]

36. After reviewing the seriousness of Superfish Adware's threat to computer security, the United States Department of Homeland Security urged immediate removal of the adware to protect users,[34] and Microsoft acted swiftly to classify Superfish Adware as a virus and delete it from infected computers.[35] In spite of the overwhelming consensus of cyber security experts, technology firms, and government agencies, Superfish continued to blame "misinformation" and point blame towards the media, downplaying the risk facing Lenovo customers.[36]

37. Ultimately, Superfish Adware was revealed to have three glaring problems that invaded the privacy of Class members and eroded the security of their electronic communication: (a) Superfish Adware intercepted Internet traffic surreptitiously, analyzed the data on external servers, and then injected advertisements in ordinary HTTP websites without Class member consent; (b) Superfish Adware intercepted Internet traffic surreptitiously, analyzed the data on external servers, and then injected advertisements into private HTTPS websites without Class member consent; and (c) Superfish Adware exposed Class members' computers to foreign attack, data interception, viruses, and data theft through their use of hacker "man-in-the-middle" attacks to undermine the

---

[32] Shira Ovide, *supra* note 11.

[33] *Id.*

[34] *Komodia Redirector with SSL Digestor fails to properly validate SSL and installs non-unique root CA certificates and private keys*, VULNERABILITY NOTES DATABASE (Revised Feb. 23, 2015) http://www.kb.cert.org/vuls/id/529496.

[35] Brad Chacos, *Bravo! Windows Defender, McAfee updates fully remove Lenovo's dangerous Superfish adware*, PCWORLD (Feb. 20, 2015 5:06 PM), http://www.pcworld.com/article/2886827/bravo-windows-defender-update-fully-removes-lenovos-dangerous-superfish-malware.html.

[36] Dan Goodin, *Superfish doubles down, says HTTPS-busting adware poses no security risk*, ARS TECHNICA (Feb. 20, 2015 4:20 PM), http://arstechnica.com/security/2015/02/superfish-doubles-down-says-https-busting-adware-poses-no-security-risk/.

security systems in Lenovo computers. This was all done with Lenovo's consent, and their callous disregard for their consumers has put the electronic information security of millions of Class members at risk.

V. CLASS ACTION ALLEGATIONS

38. Plaintiff brings this action as a class action pursuant to Rules 23(a) - (b) of the Federal Rules of Civil Procedure on behalf of himself and all others similarly situated as members of the proposed National Class, California Sub-Class, and North Carolina Sub-Class (the "Class"), defined as:

> National Class: All persons and entities in the United States that purchased the following Lenovo computers: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, U330P, U430P, U330Touch, U430Touch, U530Touch, Y430P, Y40-70, Y50-70, Z40-75, Z50-75, Z40-70, Z50-70, S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch, Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10, MIIX2-8, MIIX2-10, MIIX2-11, YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW, and E10-30 from January 1, 2014 through the present, inclusive ("Class Period").
>
> North Carolina Sub-Class: All persons and entities in North Carolina that purchased the following Lenovo computers: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, U330P, U430P, U330Touch, U430Touch, U530Touch, Y430P, Y40-70, Y50-70, Z40-75, Z50-75, Z40-70, Z50-70, S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch, Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10, MIIX2-8, MIIX2-10, MIIX2-11, YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW, and E10-30 from January 1, 2014 through the present, inclusive ("Class Period").
>
> California Sub-Class: All persons and entities in California that purchased the following Lenovo computers: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, U330P, U430P, U330Touch, U430Touch, U530Touch, Y430P, Y40-70, Y50-70, Z40-75, Z50-75, Z40-70, Z50-70, S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch, Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10, MIIX2-8, MIIX2-10, MIIX2-11, YOGA2Pro-13, YOGA2-13, YOGA2-

11BTM, YOGA2-11HSW, and E10-30 from January 1, 2014 through the present, inclusive ("Class Period").

39. Excluded from the proposed Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

40. Subject to additional information obtained through further investigation and discovery, the foregoing definitions may be expanded or narrowed by amendment or amended consolidated complaint.

41. **Numerosity**. The members of the Class are so numerous that their individual joinder is impracticable. Plaintiff is informed and believes, and on that basis alleges, that the proposed Class contains hundreds of thousands of members, potentially numbering in the millions. The precise number of Class members is unknown to Plaintiff, but that number is knowable to Defendants, and that number greatly exceeds the number to make joinder possible.

42. **Existence and Predominance of Common Questions of Law and Fact**. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, but are not limited to, the following:

A. whether Lenovo manufactured, advertised, and/or sold computers that contained Superfish Adware;

B. whether Defendants intercepted electronic communication of Class members;

C. whether Defendants violated 18 U.S.C. §2511, *et seq.* by intentionally intercepting Class members' electronic communications through the use of Superfish Adware;

D. whether Defendants engaged in unlawful or unfair practices in violation of N.C. Gen. Stat §75-1.1, *et seq.*;

E. whether Defendants engaged in unlawful or unfair practices in violation of Cal. Bus. & Prof. Code §17200, *et seq.*;

F. whether Defendants trespassed upon the property of Class members through the installation of Superfish Adware on Lenovo computers;

G. Whether Defendants trespassed upon the property of Class members through Superfish Adware's use of man-in-the-middle attacks on the security features of Lenovo computers;

H. whether Class members are entitled to, and the appropriate amount of, actual damages, statutory damages, punitive damages, and any other monetary relief; and

I. whether Class members are entitled to, and the appropriate types of equitable or declaratory relief under 18 U.S.C. §2520.

43. **Typicality**. Plaintiff's claims are typical of the claims of the members of the Class in that Lenovo manufactured and sold a computer to Plaintiff, like all other members of the Class. Plaintiff and all members of the Class are similarly affected by Defendants' wrongful conduct in violation of the Federal Wiretap Act in that their electronic communications and Internet use was intercepted by Defendants through the Superfish Adware program. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other Class members.

44. **Adequacy of Representation**. Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained counsel highly experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

45. **Superiority**. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

46. The claims asserted herein are applicable to all consumers throughout the United States who purchased Lenovo computers.

47. Plaintiff anticipates that there will be no difficulty in the management of this litigation. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

48. Adequate notice can be given to Class members directly using information maintained in Defendants' records or through notice by publication.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

VIOLATION OF 18 U.S.C. SECTION 2511, *ET SEQ.*

(On Behalf of Plaintiff and the National Class)

49. Plaintiff incorporates the previous paragraphs of this Complaint as if fully set forth herein.

50. Beginning in 2014, Lenovo intentionally intercepted or procured Superfish to intercept electronic communications of members of the National Class in violation of 18 U.S.C. §2511, *et seq*.

51. The electronic communications intercepted by Defendants were intercepted without the consent of members of the National Class. Defendants also intercepted Internet traffic that was particularly private and secured by HTTPS encryption.

52. Defendants used the Superfish Adware program to both surreptitiously intercept electronic communication and to create fake security certificates for the purposes of intercepting encrypted electronic communication.

53. Pursuant to 18 U.S.C. §2520, Plaintiff and National Class members are each entitled to the following:

A. statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000 per National Class member;

B. punitive damages in an amount to be determined by jury;

C. equitable, declaratory, and/or injunctive relief as is deemed appropriate; and

D. reasonable attorneys' fees and other costs.

SECOND CLAIM FOR RELIEF

TRESPASS TO CHATTELS

(On Behalf of Plaintiff and the National Class)

54. Plaintiff incorporates the previous paragraphs of this Complaint as if fully set forth herein.

55. At all times during the Class Period, Lenovo sold computers to members of the Class surreptitiously infected with Superfish Adware, without the knowledge or consent of Plaintiff or National Class members.

56. Plaintiff and the National Class maintained actual or constructive possession of their respective computers after they were purchased from Lenovo.

57. Defendants intentionally interfered with Plaintiff and National Class members' use and enjoyment of their computers by using Superfish Adware to spy on Internet activity, inject advertisements into web sites, use system resources, and manipulate security protocols, ultimately exposing Plaintiff and the National Class to significant risks of data theft and malicious attack.

58. As a direct result of Defendants' conduct, Plaintiff and the National Class suffered harm and impairment of their property.

THIRD CLAIM FOR RELIEF

VIOLATION OF N.C. GEN. STAT. SECTION 75-1.1, *ET SEQ.*

(On Behalf of Plaintiff and the North Carolina Sub-Class)

59. Plaintiff incorporates the previous paragraphs of this Complaint as if fully set forth herein.

60. The conduct of Lenovo, with its headquarters in North Carolina, and Superfish, as set forth in the paragraphs above, constitutes one or more acts of unfair competition or deceptive

practices within the meaning of North Carolina Unfair and Deceptive Trade Practices Act §75-1.1, *et seq.*

61. Defendants' deceptive and surreptitious installation of Superfish Adware without consent and continued violations of privacy and computer security are in and effect commerce, and are unethical, oppressive, unfair, and injurious to Plaintiff and the North Carolina Sub-Class.

62. The practices engaged in by Defendants are unlawful because they violate the Federal Wiretap Act and/or because they constitute invasion of North Carolina Sub-Class members' legally protected right to privacy under the North Carolina Constitution and other applicable law.

63. Plaintiff and the North Carolina Sub-Class have suffered injury in fact and damage to property as a result of the unfair and unlawful business practices.

64. Pursuant to §75-16 of the North Carolina Unfair and Deceptive Trade Practices Act, judgment shall be treble the amount fixed by verdict.

65. Pursuant to §75-16.1 of the North Carolina Unfair and Deceptive Trade Practices Act, reasonable attorneys' fee should be awarded as part of the Court costs.

FOURTH CLAIM FOR RELIEF

VIOLATION OF CAL. BUS. & PROF. CODE SECTION 17200, *ET SEQ.*

(On Behalf of Plaintiff and the California Sub-Class)

66. Plaintiff incorporates the previous paragraphs of this Complaint as if fully set forth herein.

67. Defendants' acts and practices, as alleged in this Complaint, constitute unlawful, unfair, and/or fraudulent business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*.

68. Defendants' deceptive and surreptitious installation of Superfish Adware without consent and continued violations of privacy and computer security are unethical, unfair, and injurious to Plaintiff and the California Sub-Class.

69. The practices engaged in by Defendants are unlawful because they violate the Federal Wiretap Act, the Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code §§22947.2-22947.4, California Penal Code §502, and/or because they constitute invasion of California Sub-Class members' legally protected right to privacy under the California Constitution and other applicable law.

70. Defendants' surreptitious installation and use of Superfish Adware are fraudulent business practices because they are likely to deceive, and did in fact deceive consumers acting reasonably under the circumstances.

71. Plaintiff and the California Sub-Class have suffered injury in fact and damage to property as a result of the unfair and unlawful business practices.

72. Plaintiff and the California Sub-Class are entitled to equitable relief including restitution of money paid, disgorgement of all profits accrued to Defendants because of their unfair, fraudulent, and deceptive practices, attorneys' fees and costs, and declaratory relief.

VII. PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, prays for relief and judgment against Defendants as follows:

A. Certification of this action as a class action and appointment of Plaintiff as the Class representative and the undersigned counsel as Class counsel;

B. An Order declaring that Defendants' conduct has violated 18 U.S.C. §2511, *et seq.*;

C. An Order awarding Plaintiff and National Class members injunctive relief, declaratory relief, statutory damages, and punitive damages against Defendants as provided in 18 U.S.C. §2520;

D. An Order declaring the actions complained of herein to be in violation of the North Carolina Unfair and Deceptive Trade Practices Act, §75-1.1, *et seq.*;

E. An Order declaring the actions complained of herein to be in violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq.*;

E. An Order declaring that Defendants trespassed upon the chattels of the Class;

F. An Order awarding Plaintiff and North Carolina Sub-Class members actual damages, punitive damages, and/or treble damages against Defendants;

G. An Order awarding Plaintiff and California Sub-Class members restitution and disgorgement of Defendants' profits;

H. Pre and post-judgment interest;

I. Reasonable attorneys' fees and costs; and

J. For such other and further relief as this Court finds just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demand a jury trial on all issues so triable.

DATED: February 24, 2015

Respectfully submitted,

By: */s/ Dhamian A. Blue*

Dhamian A. Blue
Daniel T. Blue, Jr.
Daniel T. Blue, III
Attorneys for Plaintiff
BLUE STEPHENS & FELLERS LLP
205 Fayetteville Street, Suite 300
Raleigh, North Carolina 27601
Telephone: (919) 833-1931

Fax: (919) 833-8009
E-mail:dab@bluestephens.com
State Bar No. 31405 (DAB)
State Bar No. 5510 (DTB, Jr.)
State Bar No. 27720 (DTB3)

Stuart A. Davidson
Mark J. Dearman
Holly W. Kimmel
Alex D. Kruzyk
ROBBINS GELLER RUDMAN
& DOWD LLP
120 East Palmetto Park Rd.
Suite 500
Boca Raton, FL 33432
Telephone: (561) 750-3000
Facsimile: (561) 750-3363

Carmen A. Medici
ROBBINS GELLER RUDMAN
& DOWD LLP
655 West Broadway, Suite 1900
San Diego, CA 92101-8498
Telephone: (619) 231-1058
Facsimile: (619) 231-7423